COPY-MOVE (CLONING) IMAGE FORGERY DETECTION USING WAVELETS AND PROJECTION PROFILING

Synopsis submitted in fulfillment of the requirement for the Degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & ENGINEERING

BY

MOHD DILSHAD AHMAD ANSARI
Enrollment No. 126205

Under Supervision of

Prof. Dr. Satya Prakash Ghrera

Department of Computer Science & Engineering and Information Technology,
Jaypee University of Information Technology, Waknaghat, Solan–173234,
Himachal Pradesh, INDIA

August, 2017

Table of Contents Page No.

ABSTRACT i

CHAPTER 1 Introduction 1-5
1.1 Pixel-Based Image Forgery Detection 2
1.2 Background
1.3 Problem Identification 3
1.4 Objectives of Thesis 4
1.5 Organization of Thesis 5
1.6 Specification of The System 5

CHAPTER 2 An Approach for Identification of CMFD based on Projection Profiling 7-11
2.1 Background 7
2.2 Proposed Algorithm 8
2.3 Experimental Results 9

CHAPTER 3 CMFD Using RPT and MFHWT 12-14
3.1 Background 12
3.2 Proposed Technique 12
3.3 Experimental Results 13

CHAPTER 4 DFT and RPT based CMFD 15-17
4.1 Background 15
4.2 Proposed Approach 15
4.3 Results Analysis 16

CHAPTER 5 Texture features extraction using IFLBP 18-21
5.1 Background 18
5.2 Proposed Approach 19
5.3 Results Analysis 19

CHAPTER 6 Conclusions & Future Work 22-23
6.1 Conclusions 22
6.2 Future Work 22
6.3 Publications 23
References

ABSTRACT

Digital images play an extensive role in our daily life as we are living in the digital and technical era. The images can personal or official and can be used as various important purposes such as evidence in court of law, a news item, financial record etc. Forge images are being used as original image to disguise and can be presented as false evidence. Furthermore, image processing softwares, editing tools and internet makes this process quite easy. Anyone can doctor the digital images without leaving visual clues. The activity of doctoring images is decreasing the trust-worthiness of digital images. Therefore, there is essential and effective algorithm which can detect image forgery automatically for authenticity or genuineness of the digital images.

The copy-move (cloning) is a very popular type of image forgery, which is used to create a digital image doctoring. In this technique, a specific block of image or object is copied and then pasted it to the other portion of the same image to accomplish information hiding. As the copied area move from the same image, its significant properties such as noise, color palette and texture will be well matched with the remaining part of the image. It will lead to a great remonstrance in identifying and locating the forgery regions.

Although various approaches have been proposed by number of researchers to detect copy-move image forgery (CMFD), still there are some research gaps such as false detection, high execution time and poor accuracy due to various forgery attacks. We have addressed all these issues in proposed algorithms, and new improvements have been suggested to improve the accuracy and reduce the execution time.

This thesis has been divided into six chapters. Chapter 1 introduces the concept of image forgery, classification of forgery, important characteristics and various applications of image forgery. This is followed by a literature review of copy-move image forgery detection techniques along with their merits and demerits. The method of copy-move image forgery along with major performance metrics such as Accuracy, True Positive Rate (TPR) and False Positive Rate (FPR) has been discussed. An identification of CMFD using image projection profiling with improved performance in accuracy and execution time is discussed in chapter 2.

Chapter 3 and 4 discuss robust and hybrid techniques with their performance in respect of accuracy, TPR, FPR, execution time, dimension reduction as well as after applying various attacks. We have also tested proposed algorithm on public database MICC-220. This database is having total 220 images. Total images are a combination of original image, copy-move forgery images and various attacks are also applied on forge images such as rotation, scaling, compression etc.

Chapter 5 presents texture feature extraction method, which is used in various application areas of image processing. Finally, the summery of all work along with contribution and future scope are discussed in chapter 6 followed by list of publications and references at the end.

CHAPTER # 1

INTRODUCTION

Digital image forgeries are not new to the human being but a very old problem. In the past, it was limited to art and literature but did not affect the general public. Nowadays the rapid growth of internet, digital image processing software and editing tools make this task pretty easy where a digital image can be effortlessly manipulated or forged [1]. Further, it is almost impossible for human vision system to recognize visually whether the image is original or manipulated with naked eye. There is a rapid improvement in the digital forgeries in mainstream media and on the internet [2]. This trend indicates grave vulnerabilities and decreases the trustworthiness of the digital images. Therefore, developing better techniques to authenticate the integrity and genuineness of digital images is very essential, especially taking into consideration that images can be presented as an evidence in a court of law, as news item, as a part of a medical records, or as financial documents. So, image forgery detection is one of the prime goal of digital image forensics.

Digital image forgery detection techniques are divided into active and passive techniques. In the active technique, digital image requires preprocessing of image such as watermark embedding or signature generation, which restricts their application in practice. Contrasting the watermark and signature based techniques; the passive techniques do not require any digital signature to be generated or embedded any watermark.

Passive image forgery detection approaches can be separated into five categories [2] as shown in Figure 1. Pixel based approaches identify statistical anomalies introduced at the pixel level; on the other hand, format based approaches control the statistical correlations introduced by a specific lossy compression scheme; Further, camera based approaches utilize artifacts introduced by the camera lens, sensor as well as on-chip post-processing; In physical environment based approaches, we unambiguously model and notice anomalies in the three-dimensional interaction among physical objects, light and camera; Lastly, geometry based approaches formulate dimensions of objects in the world and their positions relative to the camera.

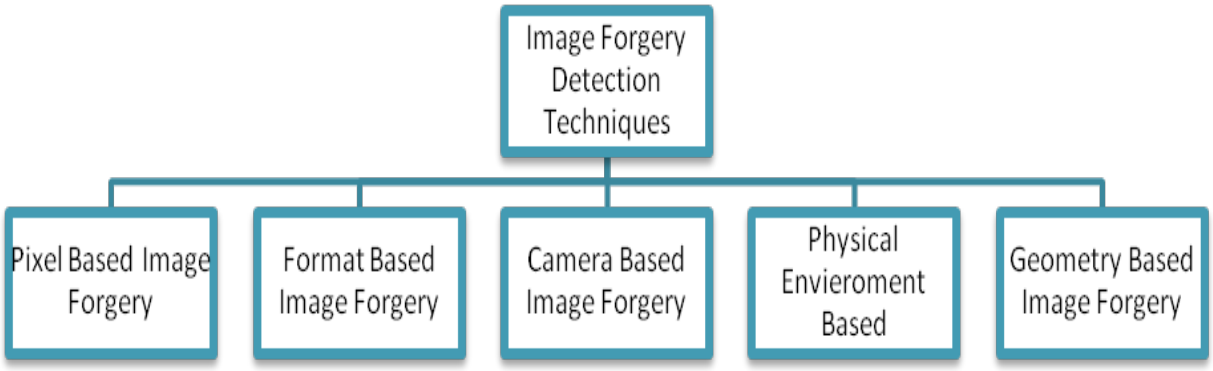

Figure1: Image forgery detection techniques

1.1 PIXEL-BASED IMAGE FORGERY DETECTION

Pixel based approaches emphasis to pixels of the image. Pixel-based approaches are also known as passive image tampering detection techniques. Further, this method is categorized into four types. In this work, we are focusing on Copy-Move image forgery. It is one of the most common forgery detection technique. Figure 2 shows the classification of pixel based forgery detection method.

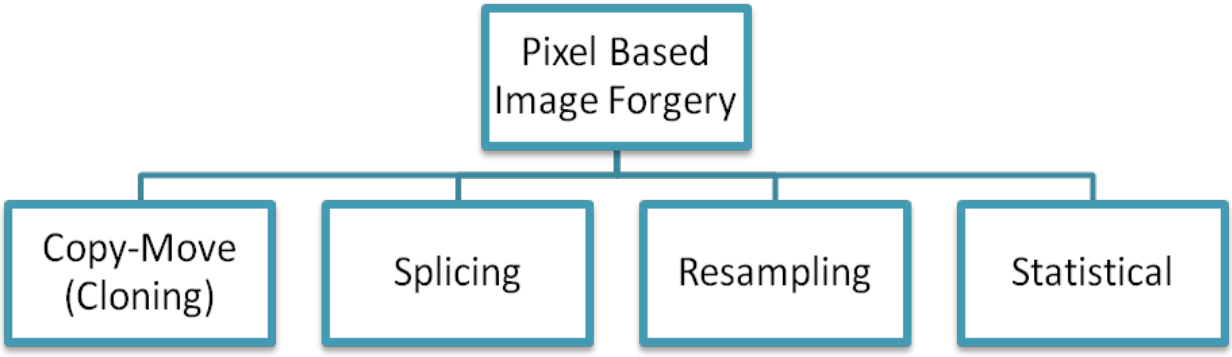

Figure 2: Pixel based image forgery

1.1.1 COPY-MOVE (CLONING)

This is one of the most common types of image forgery and this is also known as cloning. In this forgery, the area or object of image is copied and then pasted somewhere else within the image. In Figure 3, original image with six balloons and copy-move image with nine balloons.

Figure 3: Copy-move (cloning) image forgery

1.1.2 RESAMPLING (RESIZE, STRETCH, ROTATE)

For making composite for two people, it might be possible that one person have to be resized, stretch to match the relative height of other people. So this process needs to resample original image into a new sampling lattice.

1.1.3 SPLICING

This is a different type and widely used technique of image forgery. In this approach, two or more than two images will be converted into a single composite image. Suppose we have two images shown in Figure 4. We have made a composite of these two into a single image. If this is done carefully than the border between spliced are impossible to identify visually.

Figure 4: Spliced image forgery

1.1.4 STATISTICAL

The statistical model is used to detect everything from basic image manipulations such as resizing and filtering to perceptive photographic from computer generated images and detecting hidden messages.

1.2 BACKGROUND

Various algorithms have been proposed for detecting copy-move region by various researchers, some algorithms are efficient in term of detecting actual forgery region but taking too much execution time. Some algorithms are not efficient detecting forgery but having less execution time. However, very few algorithms are efficient in term of detecting forgery with less execution time but not robust in term of various attacks such as rotation, scaling, blurring, multiple copy-paste attack etc [1-5].

Firstly, Fridrich et al [1] developed a technique for detecting copy-move forgery in digital image in 2003. In this approach, the image is separated into overlapping blocks (16×16) and DCT is used for feature extraction. Further, DCT coefficients of blocks are lexicographically sorted. Moreover, similar blocks are identified and copy move region is detected. Authors have also carried out retouching operations in the image but no robustness test has been performed.

Next, Popescu et al [2] initiated a technique for exposing digital forgeries by detecting duplicated image regions in 2004. Principal component analysis (PCA) is applied on fixed size image blocks (16×16, 32×32). Further, eigenvalues and eigenvectors have been calculated of each block. Moreover, lexicographical sort is applied and duplicated regions have been detected. This technique provides better results compare to fridhrich methods. This technique is able to detect duplicate region if the image is compressed or noisy.

Huang et al [3] proposed copy-move forgery in digital images using SIFT algorithm in 2009. In this paper, authors have introduced SIFT (Scale Invariant Feature Transform) algorithm using feature matching. Further, these features are matched to detect forgery region.

Gouhui Li et al [4] introduced a sorted neighborhood technique for detecting duplicate region based on DWT and SVD in 2007. First DWT is used to decompose image into four sub-bands. Further, low frequency sub band is chosen for further processing. Moreover, singular value decomposition (SVD) is used to extract feature vector on reduced dimension representation. Lexicographical sort is applied on singular value vector and similar vectors are nearby. These vectors are matched and forged region detected. They have used gray scale as well as color images for detecting duplicate region.

Amerini et al [5] detected the duplication in images and also estimated the transformation by RANSAC. They developed g2NN nearest neighbor searching for multiple copy paste detection. Further, various methods have been proposed to detect copy-move (cloning) image forgery [6-21, 23-27, 45-47].

1.3 PROBLEM IDENTIFICATION

In this thesis, we have focused to design robust algorithms which are able to detect forgery with less execution time and also able to detect forgery on images subjected to scaling, rotation, blurring, and multiple copy-paste attacks. We have focused on the following issues:

- *In the literature survey of image forgery, we have found that the number of existing approaches, which are not able to detect actual forgery region. So, the false matches are the major limitation. Detecting actual region with good accuracy rate is the challenging tasks. We have addressed this issue and proposed an algorithm based on projection profiling.*
- *We have processed the image block by block and extracted the feature vector for each block then compared similar the feature vector to find the possible duplication. The extraction process will take lot of computational time so improving computational time is other major challenge of this research domain. We have suggested a hybrid algorithm based on direct fuzzy transform and ring projection which reduces the execution time as well as improve the accuracy.*

1.4. OBJECTIVES OF THESIS

Image processing software's, editing tools and internet makes image forgery process quite easy. Anyone can doctor images without leaving any visual clues. Therefore, there is necessity of some effective algorithm which can detect image forgery automatically with good accuracy rate. Objective of the thesis are given as follows:

- *To propose a robust and efficient forgery detection algorithm, which is able to detect forgery region successfully. Also reduce the false matches and suggest new improvement in the accuracy rate.*
- *To develop a lightweight and fast technique for detecting copy-move image forgery. The algorithm will take less execution time for detecting copy-move region compare to existing approaches.*
- *To introduce a hybrid scheme. Which provide better result compare to other reported algorithms if various attacks are applied. And able to detect copy-move forgery region accurately with less execution time.*

- *To propose an efficient scheme for extracting feature from digital image, further these extracted feature vector can be used is many application areas of image processing including forgery detection.*

We design a forgery detection technique with less execution time and robust to various forgery attacks. Proposed algorithms obtain the several objectives and identified number of problems in existing forgery detection techniques and their solutions are proposed.

1.5. ORGANIZATION OF THE THESIS

The thesis has been organized into six chapters as follows:

In chapter 1, we have provided the introductory part of the thesis as well as Literature review and background. In chapter 2, we have presented an approach for identification of copy-move image forgery based on projection profiling for reducing the execution time. In chapter 3, a hybrid scheme for copy-move image forgery detection using ring projection and modified fast discrete haar wavelet transform is discussed. Chapter 4 presents a copy-move image forgery detection using direct fuzzy transform and ring projection. This algorithm is efficient in term of accuracy of detecting forgery as well as reducing the execution time. Further, chapter 5 demonstrates a texture features extraction technique using intuitionistic fuzzy local binary pattern. Finally, the conclusions and future scope are discussed in chapter 6. List of publications and references are depicted at the end.

1.6. SPECIFICATION OF THE SYSTEM FOR TESTING OF ALGORITHM

PC configuration: Intel(R) Core(TM) i3 CPU M370, 2.40 GHz, 4 GB of RAM.

Operating System: Microsoft Window 7 Ultimate 64 bit

Software: MATLAB 10.

Tool: Image processing Tool

CHAPTER # 2

AN APPROACH FOR IDENTIFICATION OF COPY-MOVE IMAGE FORGERY BASED ON PROJECTION PROFILING

An image forgery is a common problem which causes the negative impact on society. In the past, it did not affect the general public because the sophisticated image processing software and editing tools were not easily available. Thus, the rapid growth of the image processing software makes this task pretty easy. If it is done with care then it is very difficult for human vision system to distinguish visually whether the image is original or forged. Therefore, the authenticity of an image is a necessity of today's digital era. Further, copy-move image forgery is the most common and very popular type of image forgery in which an area or object is copied and pasted at some other places within the same image in order to hide some important features of the image[35].

2.1. PROPOSED METHOD

Algorithm: Fast CMFD

Step 1:- Convert an image I (color/gray) of order (M,N) into binary image J.
Step 2:- Let h(j) and v(i) be the horizontal and vertical projection profile of J respectively, They are defined as

$$h(j) = \sum_{i=1}^{M} \boldsymbol{J}(i,j) \qquad and \qquad v(i) = \sum_{j=1}^{N} \boldsymbol{J}(i,j).$$

Step 3:- Consider a moving average filter of order L with impulse response

$$r(n) = \frac{1}{L}\sum_{l=0}^{L-1} \boldsymbol{\delta}(n-l),$$

where L<<min (M,N), n= no of samples, l=0,1, 2…n.

Step 4:- Pass the horizontal h and vertical projection profile v through this filter and let h' and v' be the outputs of this filter as given below,

$$h'(j) = \sum_{k=1}^{L} r(k)h(j-k) \qquad and \qquad v'(i) = \sum_{k=1}^{L} r(k)v(i-k).$$

Step 5:- Find the means of these outputs of the filter

$$m_h = \frac{1}{N}\sum_{j=1}^{N} h'(j) \qquad and \qquad m_v = \frac{1}{M}\sum_{i=1}^{M} v'(i).$$

Step 6:- Search for the corner indexes of the rectangular region of copy-move part.
Let, $h_s = h_e = v_s = v_e = \phi$, where ϕ is a null set.

$for\ j \rightarrow 1{:}N$
$if\ h'(j) < m_h$
$h'(j) = 1$
$else$
$h'(j) = 0$
$h''(j) = h'(j) - h'(j-1)$
$if h''(j) = 1$
$hs = [hs, j]$
$if h''(j) = -1$
$he = [he, j]$
end
$for\ i \rightarrow 1{:}M$
$if\ v'(i) < m_v$
$v'(i) = 1$
$else$
$v'(i) = 0$
$v''(i) = v'(i) - v'(i-1)$
$if v''(i) = 1$
$vs = [vs, i]$
$if v''(i) = -1$
$ve = [ve, i]$
end

Step 7:- Identifying the rectangular regions of the copy-move part of the image I.

$\boldsymbol{R_1} = \mathbf{I}(hs(1,1){:}\ he(1,1), vs(1,1){:}\ ve(1,1))$
and
$\boldsymbol{R_2} = \mathbf{I}(hs(1,2){:}\ he(1,2), vs(1,2){:}\ ve(1,2))$

where**, R1** and **R**2 are the matched regions.

2.2 EXPERIMENTAL RESULT & DISCUSSION

We have proposed a new method for image forensics based on projection profiling. As the block-based copy-move forgery detection methods are computationally intensive, any improvement in execution time will help in checking forgery from the given image. The proposed method successfully addresses the issue and noticeably faster than the existing

methods. To check the robustness of our proposed approach, it has been performed on more than 50 images. The accuracy of proposed algorithm is 88% which shows new improvement compare to existing approaches [1, 2]. The results show that the proposed approach is able to detect copy-move region effectively and new improvements have been suggested in computational time shown in Table 1.

Figure 5: (*a*) Original image (*b*) Forged image and (*c*) Detected region of copy-move forgery.

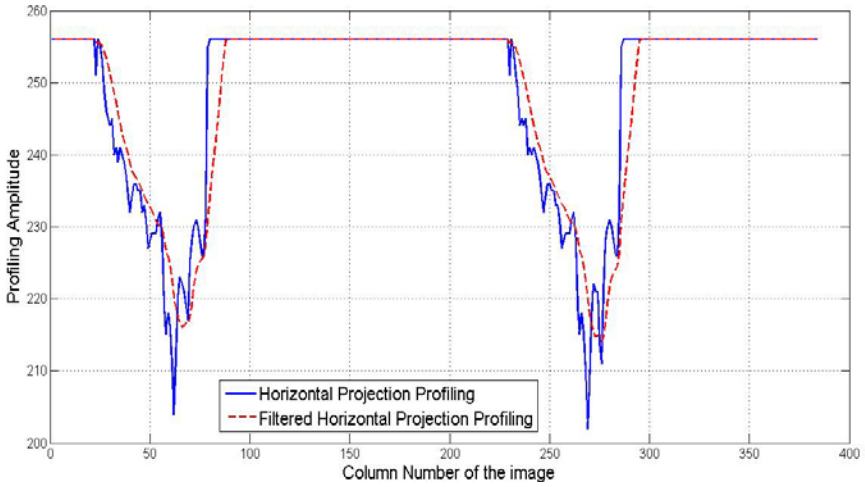

Figure 6: Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 5(*b*).

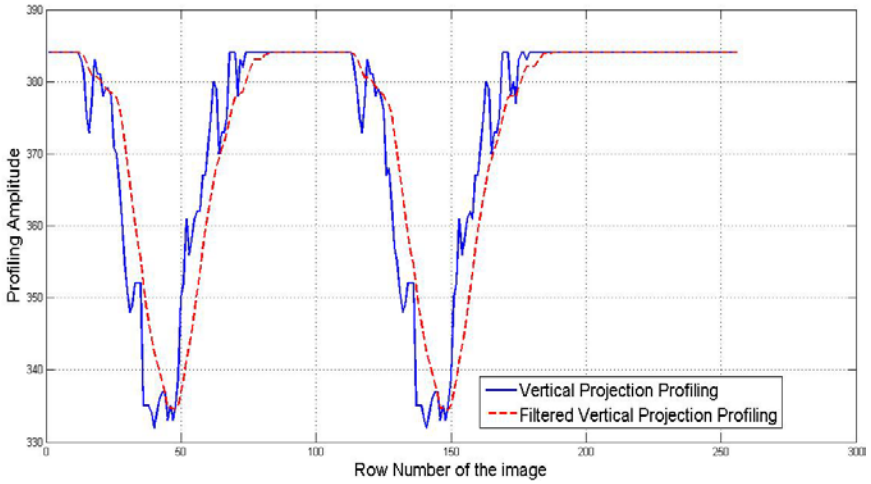

Figure 7: Vertical projection profile and filtered vertical projection profile for the image shown in Figure 5(*b*).

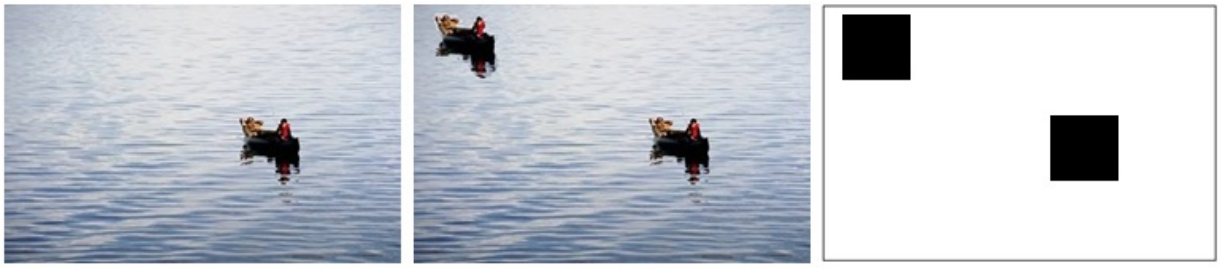

Figure 8: (*a*) Original image (*b*) Forged image and (*c*) Detected region of copy-move forgery.

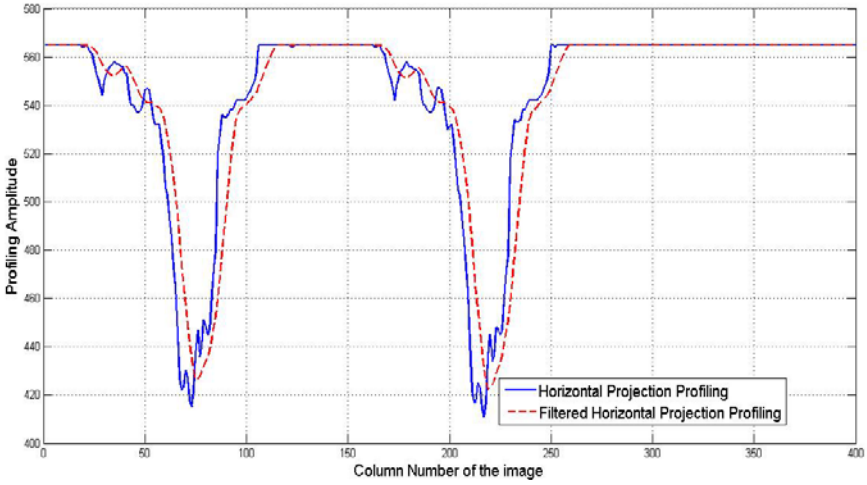

Figure 9: Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 8(*b*).

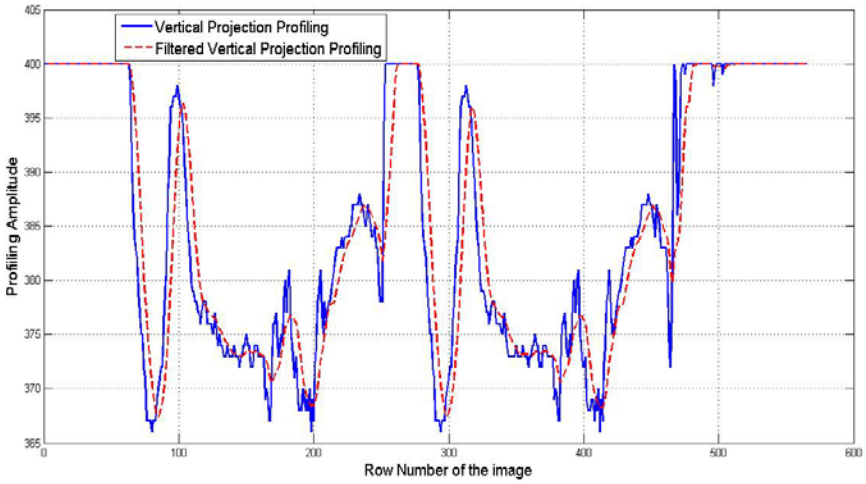

Figure 10: Vertical projection profile and filtered vertical projection profile for the image shown in Figure 8(*b*).

Table 1 Copy-move forgery detection execution time in seconds

Image Name	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7
Image Size	128×128	256×256	384×384	424×424	512×512	656×656	832×832
Xiaofeng et. al[43]	4.96	39.70	171.09	239.48	478.109	1259.35	1308.25
Proposed Method	3.29	4.27	4.81	5.33	5.69	6.12	6.84

CHAPTER # 3

COPY-MOVE IMAGE FORGERY DETECTION USING RING PROJECTION AND MODIFIED FAST DISCRETE HAAR WAVELET TRANSFORM

In recent years, the popularity of digital cameras, smart phones and tablets has made the acquisition of digital images easier. In addition to that, modern photo editing software package such as Photoshop makes it relatively easy to create digital image forgeries, on which people almost cannot perceive the difference between the original image and its tampered version. There is speedy enlarge in digitally manipulated image forgeries in social media and on the internet. These kinds of activities are decreasing the credibility of the digital image, so there must be some algorithms which can provide the authenticity of digital images.

3.1 PROPOSED ALGORITHM

We propose a boosting scheme to reduce the computational overhead and number of estimated blocks each time and it turns out to decrease time and memory efficiency dramatically [33-34, 36-37]. The proposed method has been applied on gray images as follows:

Algorithm: CMFD using MFHWT

Step 1:- Read the input image, if the input image is RGB, then converts it into gray scale version by I = 0.228R + 0.587G + 0.114B.

Step 2:- Apply MFHWT up to specified level 'L' to the gray image

Step 3:- Overlapping blocks of size b×b are created in the LL_L image with one pixel shifting and the total number of overlapping blocks is given by $Novr = (M/b + M/b^2) \times (N/b+ N/b^2)$.

Step 4:- If the contrast value of each overlapping b×b is less than the predefined ′CTR′, then we ignore it, otherwise we apply the following steps:

(a) Transform each overlapping b × b into a 1 – D RPT vector of size R + 1.

(b) The feature vectors extracted from Step (a) are arranged in a matrix, denoted as A.

(c) In the mean while, form matrix P of two columns for storing top-left co ordinates.

Step 6:- Apply lexigraphical order to the matrix A so that similar blocks are consecutively sorted.

Step 7:- For every adjacent rows of matrix A,

(a) Compute the normalized correlation co-efficient between the pair of sorted rows

(b) If the computed correlation co-efficient exceeds a preset threshold value ′C′t, then extract the corresponding blocks position from the matrix P, and marked the location of these forged blocks are in the original image by setting pixel values to zero.

Step 8: Copy-move region are identified.

3.2 RESULT ANALYSIS

To determine the performance of proposed method and its quality, a realistic database can be constructed. We have composed a database of 100 images, where 50 images are forged and 50 images are original. This database is having different type of image format and various resolutions like 256×256, 512×512, 640×480 etc. The forged images are constructed with the help of Photoshop, in which the forge area or object is randomly selected and pasted into the same image. The new improvement has been suggested in accuracy and computational time as shown in Table 2, Table 3.

Figure 11: (a) Original image, (b) Forged image, (c) Forgery detection with CTR=2 and (d) Forgery detection with CTR=1.

Table 2: Accuracy Results

Forgery Type	No. of Images	Identified Correctly	Identified Incorrectly	Accuracy
Normal Images (50)	100	95	5	95%
Forgery with Blurring (25)	100	89	11	89%
Forgery with Rotation (25)	100	87	13	87%
Forgery with Multiple (25)	100	92	8	92%
Total	400	363	37	90.75%

Table 3: Accuracy Comparison on Test Images

Images	Proposed Method	Method in [17]	Method in [45]	Method in [1]
Deer	87.85	84.15	67.17	68.58
Extension	76.74	72.15	25.54	40.25
Red Tower	94.26	91.75	55.49	70.16
Tree	81.92	77.13	61.02	57.91
Truck	80.25	74.06	57.64	55.53
CRW	65.84	62.45	20.81	24.00

CHAPTER # 4

COPY-MOVE IMAGE FORGERY DETECTION USING DIRECT FUZZY TRANSFORM AND RING PROJECTION

Forgeries were extremely hard when computers, digital camera and smart phone are not easily available. Nowadays, the recognition of smart phones and digital cameras has made the task acquirement of digital images easier. Moreover, current photo editing tools such as Photoshop makes it comparatively easy to produce digital image forgeries. Additionally, humans essentially cannot distinguish the dissimilarities between the original and its forged image. The Cloning image forgery is the very popular type of technique; perform to create a digital image doctoring. Additionally, in which a specific block of image or object is copied and then pasted it to the other portion of the same image to accomplish information hiding. As the copied region move from the same image; its important properties such as noise, color palette as well as texture, will be well matched with the remaining part of the image. It will lead to a great remonstrance in identifying and locating the forgery regions.

4.1 PROPOSED ALGORITHM

We propose a compromise scheme to decrease the execution time and number of estimated blocks every time and it turns out to decrease the time and memory drastically [36-40]. Proposed algorithm is able the increases accuracy and also robust to various forgery attacks. The proposed model is given below:

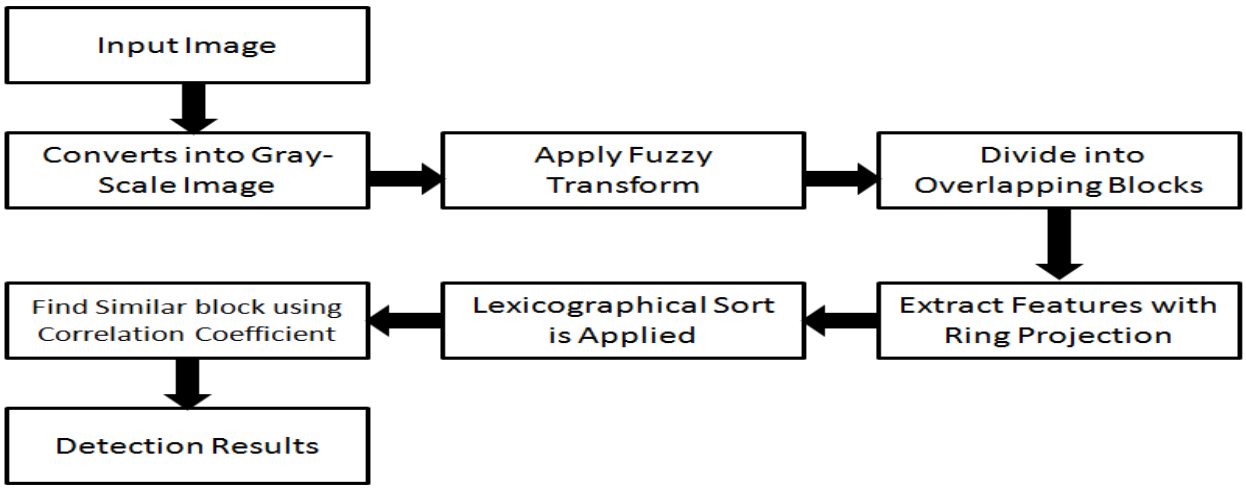

Figure 12: Proposed model

4.2 RESULT ANALYSIS

Accuracy, true positive rate (TPR), false positive rate (FPR) was calculated to prove the robustness of proposed algorithm. The experiments were carried out on MATLAB R2010a, RAM 4 GB and core i3 processor. The database of 100 images was composed where 50 images were original and 50 were tempered. This database is having different types of image format (.jpg, .png and .tiff) and various resolutions like 256×256, 512×512, 640×480 etc. The forged images are constructed with the help of Photoshop in which the forge area or object is randomly selected and pasted into the same image. Furthermore, one public database MICC-F220 [44] also used for the comparative analysis of proposed algorithm with other reported techniques. This database is containing total 220 images out of them 110 are original and 110 are forged. Additionally, various types of attacks such as scaling, rotation and blurring were also applied on tempered images of both databases to check the robustness of proposed algorithm.

Figure 13: Forgery detection on MICC-220 Database (a) Original image, (b) Forgery image of (a), (c) Fuzzy transform image and (d) Forgery detection

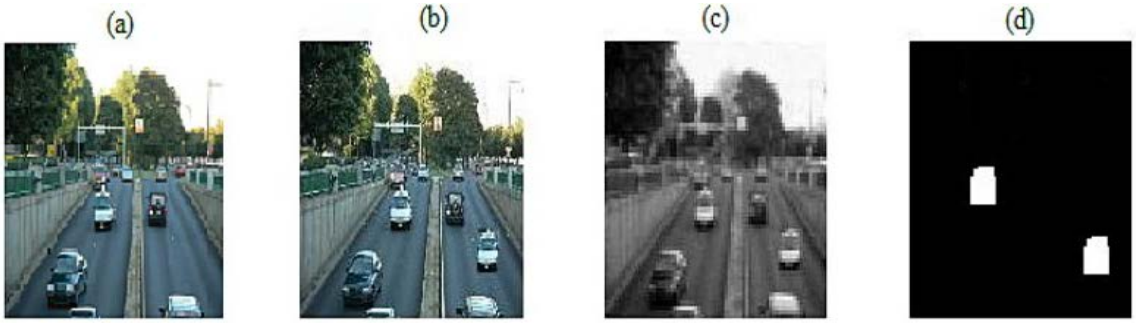

Figure 14: Forgery detection on MICC-220 Database (a) Original image, (b) Forgery image of (a), (c) Fuzzy Transform image and (d) Forgery detection

Figure 15: Forgery detection on MICC-220 Database (a) Original image, (b) Forgery image of (a), (c) Fuzzy Transform image and (d) Forgery detection

Table 4: Accuracy Results

Block-Size	No. of Images	Identified Correctly	Identified Incorrectly	Accuracy
4×4	100	94	6	94%
8×8	100	93	7	93%
16×16	100	91	9	91%
32×32	100	87	13	87%
Total	400	365	35	91.25%

Table 5: TPR, FPR and Execution Time in seconds Comparison for Each Method on MICC-F220

Methods	TPR	FPR	Execution Time (S)
Fridrich et. al[1]	89	84	294.96
Popescu et. al [2]	87	86	70.97
Pan et. al [46]	89	1	10.00
Proposed Method	90	34	3.80

CHAPTER # 5

TEXTURE FEATURES EXTRACTION USING INTUITIONISTIC FUZZY LOCAL BINARY PATTERN

The primary research on visual inspection has demonstrated that the LBP features were efficiently applied in surface defect detection. Afterwards, BP based features are also applied in wood quality discrimination. Lately, such features have been used in automatic defect detection as well as in remote sensing. Various studies have demonstrated the BP based feature extraction techniques which are advisable for content based image retrieval (CBIR) while the LBP based techniques utilized discriminative model for image ranking from text queries. Furthermore, in the field of face recognition, the LBP is identified as a highly proficient texture representation technique [28-30, 47]. For example, it is proficiently employed in invariant face recognition, recognition of facial expressions and face authentication. Wonderful results are achieved from its various application of biomedical imaging including classification of protein images, video endoscopy, and computer aided neuroblastoma prognosis system [48].

5.1 PROPOSED ALGORITHM

Algorithm: Feature Extraction using IFLBP

Step 1:- Consider image as input.

Step 2:- . Pick out the 3x3 local neighborhoods for each pixel from the input image

Step 3:- Fix a threshold value T.

Step 4:- Consider the two fuzzy rules R1 and R2 to describe the relation between the intensity values of the peripheral pixels i and the central pixel n of a 3x3 neighborhood.

R1 : if g_i<=g_c then d_x=0

R2 : if g_i>g_c then d_x=1

Step 5: Calculate the 3x3 neighborhood and find the contribution C_IFLBP of each LBP code in a single bin of the IFSLBP histogram.

Step 6: Combine all the IFLBP values of each pixel it creates an IFLBP image.

Step 7: The histogram for the IFSLBP image will be displayed to show the occurrences of different IFLBP codes in the image.

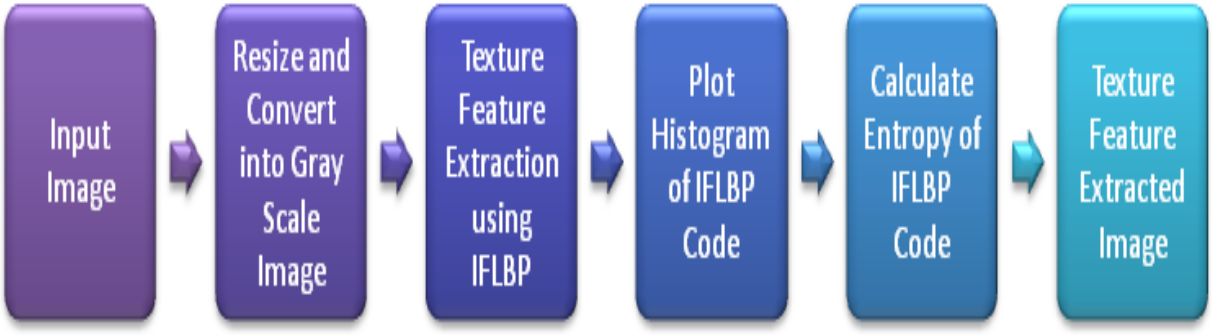
Input Image
Resize and Convert into Gray Scale Image
Texture Feature Extraction using IFLBP
Plot Histogram of IFLBP Code
Calculate Entropy of IFLBP Code
Texture Feature Extracted Image

Figure 16 : Proposed model

5.2 EXPERIMENTAL RESULTS

It can be observed that Keramidas et al [30] method had zero values for some bins out of 255 bins. However, proposed method's histograms do not have bins with zero values and there are more spikes, though limited in magnitude. This indicates that proposed method is more informative than Keramidas method [30].

Entropy is a measure of uncertainty associated with the random occurrences, normally considered as the measure of `disorder'. Pal and Pal entropy [42] is a statistical measure of randomness which is carried out to describe the texture of a given image.

we apply proposed IFLBP approach on various images as shown in Figure 17-18 of size 256×256 to calculate the histograms feature vector for different threshold values and varying hesitation (h€ [0,1]) as well as computed entropies from these histograms, finally the results are shown in Tables 6 to 7. We can examine from these tables that the maximum entropy obtained in Table 6 for the T2=, T=16, T=14, T=20 are at h=0.1, for T=10 are at h=0.3. We follow the same procedure for remaining images; results are shown in Tables 7 and Figure 18 respectively. Therefore, the entropies obtained by proposed method are always greater than the entropies obtained by existing methods. We plot the histograms of IFLBP codes of every image where we have found the maximum entropy as shown in Figure 17-18. From these histograms, we can observe that the IFLBP histograms do not have bins with zero values. In addition, the IFLBP features of all images are more informative than existing features.

Table 6. The entropy values at different threshold and hesitation for JUIT Logo image

Methods	Hesitation (h)	Threshold (T)				
		2	6	10	14	20
Keramidas et al.[31]	0.0	0.74	0.70	0.68	0.67	0.62
Proposed	0.1	**2.70**	**2.70**	2.70	**2.70**	**2.70**
	0.3	2.69	2.69	**2.70**	2.70	2.70
	0.5	2.68	2.68	2.68	2.68	2.68
	0.7	2.63	2.63	2.63	2.63	2.63
	1.0	2.18	2.16	2.14	2.13	2.12

Table 7. The entropy values at different threshold and hesitation for Lena image

Methods	Hesitation (h)	Threshold (T)				
		2	6	10	14	20
Keramidas et al.[31]	0.0	1.77	1.68	1.13	0.60	0.49
Proposed	0.1	**2.67**	2.69	2.69	2.70	2.70
	0.3	2.66	**2.69**	**2.70**	**2.70**	**2.70**
	0.5	2.67	2.69	2.70	2.70	2.70
	0.7	2.66	2.69	2.70	2.70	2.70
	1.0	2.67	2.69	2.70	2.70	2.70

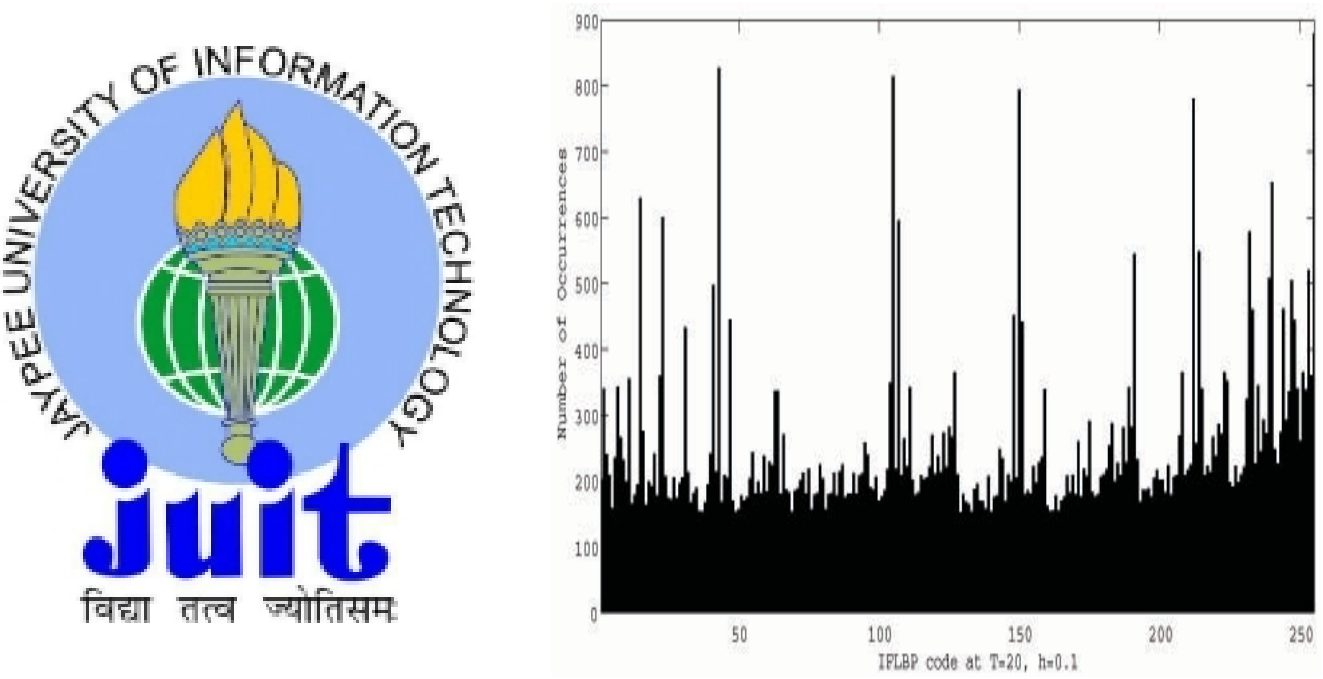

Figure 17: Histogram Plot of IF LBP Codes for JUIT Logo Image

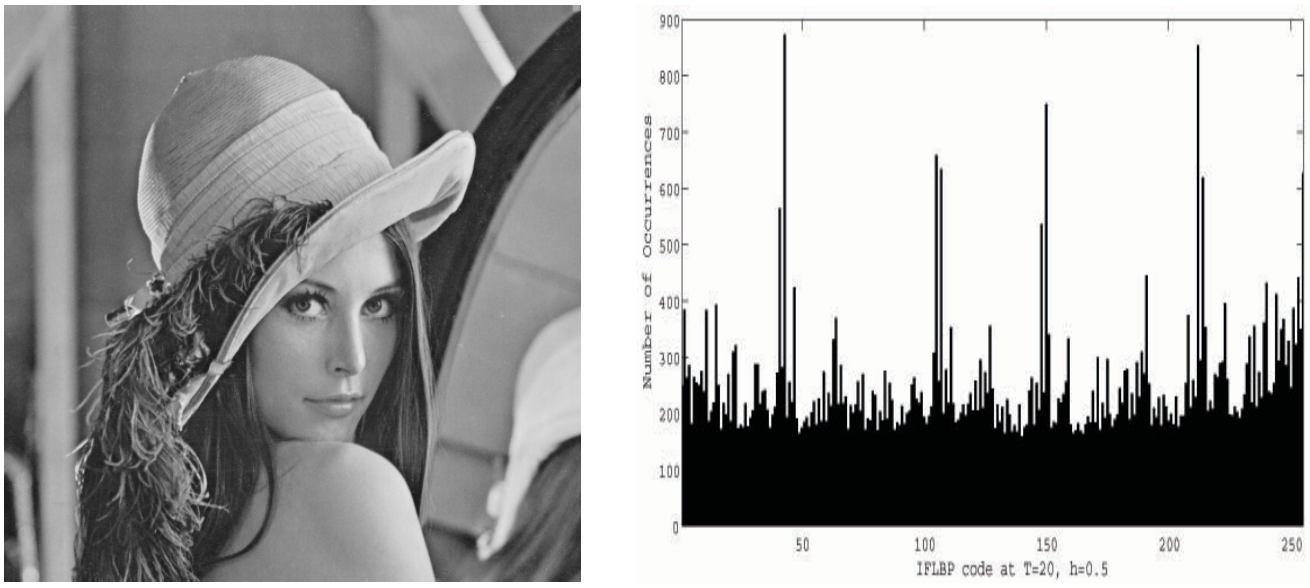

Figure 18: Histogram Plot of IF LBP Codes for Thyroid Image

CHAPTER # 6

CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSIONS

This thesis emphasizes on copy move image forgery detection techniques. New approaches have been proposed to address open issues such as accuracy and execution time.

Chapter 2 presents an approach for identification of copy-move image forgery based on projection profiling. A fast algorithm for detecting copy move region which is tested on more than 50 images of various sizes such as 256×256 and 512×512 etc. The accuracy of the proposed algorithm is 88%. The execution time is comparative less with the various existing algorithms. The new improvements have been suggested in terms of accuracy as well as execution time compare with existing techniques.

In chapter 3, we have designed a hybrid method for copy-move image forgery detection using ring projection and modified fast discrete haar wavelet transform. It is used to detect copy-move image forgery by comprises scheme of haar wavelet and RPT, the time efficiency can be greatly improved. The accuracy of proposed method is 90.75% and execution time is also improved.

In chapter 4, we have developed a direct fuzzy transform and ring projection based copy-move image forgery detection method for detecting copy-move forgery. This approach is successfully able to improve the accuracy and reduce the execution time and robust to attacks such as rotation, scaling and blurring etc. The accuracy is 91.25%.

Chapter 5 presents the texture features extraction method using intuitionistic fuzzy local binary pattern. These extracted features are found more informative and efficient compare to other reported algorithms. This technique can be used in many applications areas of image processing.

6.2 Future Work

In future, proposed algorithm can be tested on colour images and texture feature extraction algorithm can be used to extract feature vector. Further, these features may be used to detect forgery as well as the other image processing areas such as pattern recognition, medical imaging, face detection and so on.

6.3 LIST OF PUBLICATIONS

Journal Papers Published

1. **Mohd Dilshad Ansari,** Satya Prakash Ghrera and Vipin Tyagi, "Pixel-Based Image Forgery Detection: A Review", *IETE Journal of Education,* Vol. 55(1), 2014. [Published By **Taylor & Francis**] ***Citations: 30***

2. **Mohd Dilshad Ansari,** Satya Prakash Ghrera and Mohd Wajid "An Approach for Identification of Copy-Move Regions based on Image Projection Profiling", *Journal of Science and Technology,**(JST),* **Pertanika,** Vol. 25(2), 2017. **[**Indexed in **Scopus, Thomson Reuters]** ***Citations: 3***

3. **Mohd Dilshad Ansari** and Satya Prakash Ghrera "Intuitionistic Fuzzy Local Binary Pattern for Features Extraction", *International Journal of Information and Communication Technology **(IJICT),*** **Inderscience** [Indexing in **Scopus, ACM**] **(**Online Available) **DOI:** 10.1504/IJICT.2018.10005094. ***Citations: 5***

Journal Papers under Review

4. **Mohd Dilshad Ansari** and Satya Prakash Ghrera "Direct Fuzzy Transform and RPT Based Copy-Move Image Forgery Detection", *Iranian Journal of Science and Technology,* **Springer.** [Indexed in **SCI, Scopus] (Under Review)**

5. **Mohd Dilshad Ansari** and Satya Prakash Ghrera "Copy-Move Image Forgery Detection using Ring Projection and Modified Fast Discrete Haar Wavelet Transform", *International Journal on Electrical Engineering and Informatics,* **Malaysia.** [Indexed in **Scopus**] (**Under Review**)

6. **Mohd Dilshad Ansari,** Satya Prakash Ghrera and A.R. Mishra "Texture Feature Extraction using Intuitionistic Fuzzy Local Binary Pattern", *Journal of Intelligent & Fuzzy System,* **IOS Press. [**Indexed in **SCI**, **Scopus**] (**Under Review**)

Conference Paper Published

7. **Mohd Dilshad Ansari** and Satya Prakash Ghrera "Feature Extraction Method for Digital Images Based on Intuitionistic Fuzzy Local Binary Pattern" ***5th IEEE** International Conference on System Modeling & Advancement in Recent Trends **(SMART- 25-27 Nov 2016)**, pp. 345-349, 2016. TMU, Moradabad, Uttar Pradesh, India.* [Indexed in **Scopus, ISI**]

8. **Mohd Dilshad Ansari** and Satya Prakash Ghrera "On Copy Move Image Forgery Detection using Modified Fast Discrete Haar Wavelet Transform" ***4th IEEE** International Conference on Computing for Sustainable Global Development **(IndiaCom- 1-3 March 2017)** Bharati Vidhyapeeth, New Delhi, India.* **(Accepted & Presented)** [Indexed in **Scopus, IET**]

References

1. Fridrich, J., Soukal D., & Lukas, J. “Detection of copy move forgery in digital images,” Proceedings of the Digital Forensic Research Workshop, August 2003, pp.5-8.
2. Popescu, A. C. & Farid, H. “Exposing digital forgeries by detecting duplicated image regions”, Technical Report, TR2004-515, Dartmouth College, 2004.
3. Huang, H., Guo , W., & Zhang ,Y. “Detection of copy-move forgery in digital images using SIFT algorithm,” Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-276, 2008.
4. Li, G., Wu, Q., Tu, D., & Sun, S. “A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD,” International Conference on Multimedia and Expo, China, pp.1750-1753, 2007.
5. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. “A SIFT-based forensic method for copy move attack and transformation recovery”, IEEE Transactions on Information Forensics and Security Vol.6 (3), pp.1099-1110, 2011.
6. Lin, S. D., & Wu, T. “An Integrated Technique for Splicing and Copy-move Forgery Image Detection,” 4th International Congress on Image and Signal Processing (CISP), vol. 2, pp. 1086-1090. IEEE, 2011
7. Kang, X., & Wei, S, “Identifying Tampered regions using singular value decomposition in Digital image forensics,” International Conference on Computer Science and Software Engineering, Vol. 3, pp. 926–930, 2008.
8. Ghorbani, M., Firouzmand, M., & Faraahi, A. “DWT-DCT (QCD) Based Copy-move Image Forgery Detection”, 18th International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 1-4, 2011.
9. Farid, H. “A survey of image forgery detection,” IEEE Signal Process. Mag., vol. 26(2), pp. 16–25, 2009.
10. Redi, J. A., Taktak, W., & Dugelay, J. L. “Digital Image forensic: a booklet for beginners” Multimedia tools and application, Vol. 51(1), pp.133-162, 2011.
11. Lin, H. J., Wang, C. W., & Kao, Y. T. “Fast Copy-Move Forgery Detection,” WSEAS Trans. Signal Process, Vol. 5(5), pp.188–197, 2009.
12. Luo, W., Huang, J., & Qiu, G. “Robust detection of region-duplication forgery in digital image,” 18th International Conference on Pattern Recognition (ICPR2006), Vol. 4, pp. 746-749, 2006.

13. Zhang, J., Feng, Z., & Su, Y. “A New Approach for Detecting Copy-Move forgery in Digital Images”. International Conf. on Comm. Sys., Singapore, pp. 362–366, 2008.
14. Kang, L., Cheng, X. P. “Copy-move Forgery Detection in Digital Image,” International Congress on Image and Signal Processing (CISP2010) IEEE Computer Society, pp. 2419-2421. 2010.
15. Qu, Z., Qiu, G., & Huang, J. ”Detect Digital Image Splicing with Visual Cues” International workshop on information hiding, Springer, Berlin, Heidelberg, pp 247-261, 2009
16. Lin, Z., He, J., Tang, X., & Tang, C. K.” Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis” Pattern Recognition, Vol.42 (11), pp. 2492–2501, 2009.
17. Huang, Y., Lu, W., Sun, W., & Long, D. "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206 (1), pp. 178-184, 2011.
18. Qiao, M., Sung, A., Liu, Q., & Ribeiro, B. "A novel approach for detection of copy-move forgery", Fifth International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2011), pp. 44-47, 2011
19. Ryu, S. J., Lee, M. J., & Lee, H. K “Detection of copy-rotate-move forgery using zernike moments,” International Workshop on Information Hiding, Vol.6387, pp.51-65, 2010.
20. Chuang, W. H., Swaminathan, A., & Wu, M. “Tampering identification using empirical frequency response,” International Conference on Acoustics, Speech, and Signal Processing (ICASSP’09), pp. 1517–1520, 2009.
21. Zimba, M., & Xingming, S. “DWT-PCA (EVD) based copy-move image forgery detection”, International Journal of Digital Content Technology and its Applications, Vol.5 (1), pp.251-258, 2011.
22. Gonzalez, R.C., Woods, R.E. “Digital Image Processing”, 2nd edn. (2002)
23. Zhang, C., Zhang, H. “Exposing Digital Image Forgeries by Using Canonical Correlation Analysis”, International Conference on Pattern Recognition (ICPR), pp.838–841, 2010
24. Bayram, S., Sencar, H. T., & Memon, N. “An efficient and robust method for detecting copy-move forgery”, International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1053-1056, 2009.

25. Bayram, S., Sencar, H. T., & Memon, N. "A survey of copy-move forgery detection techniques," IEEE Western New York Image Processing Workshop, Rochester, NY, pp. 538-542, 2008.
26. Popescu, A. C. & Farid, H., "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, Vol. 53 (10), 3948-3959, 2005.
27. Popescu, A.C., Farid, H. "Exposing digital forgeries by detecting traces of resampling". IEEE Transactions on Signal Processing, Vol.53 (2), pp.758–767, 2005.
28. A. Barcelo, E. Montseny, and P. Sobrevilla, "Fuzzy Texture Unit and Fuzzy Texture Spectrum for texture characterization", Fuzzy Sets and System, Vol.158 (3), pp.239-252, 2007.
29. Ahonen, T., & Pietikäinen, M. "Soft histograms for local binary patterns", Finnish Signal Processing Symposium, Vol. 5 (9), pp. 1-5, 2007.
30. Keramidas, E., Iakovidis, D., & Maroulis, D. "Fuzzy binary patterns for uncertainty-aware texture representation", Electronic Letters on Computer Vision and Image Analysis, Vol.10 (1), pp.63-78, 2011.
31. Zadeh, L.,"Fuzzy Sets", Journal of Information and Control,Vol.8(3),pp.338-353, 1965.
32. Mahdian, B., & Saic, S. "Detection of copy-move forgery using a method based on blur moment invariants", Forensic science international, vol. 171(2), pp. 180-189, 2007.
33. Roeser, P. R., & Jernigan, M. E."Fast Haar Transform Algorithm", IEEE Transactions on Computer", Vol. 31 (2), pp.175–177, 1982.
34. Kaiser, G."The Fast Haar Transform: Gateway to Wavelet", IEEE Potentials, Vol.17 (2), pp.34-37, 1998.
35. Wajid, M., Abdullah, M. W., & Farooq, O. "Imprinted Braille-character pattern recognition using image processing techniques" International Conference on Image Information Processing (ICIIP), pp. 1-5, 2011.
36. Tang, Y. Y., Cheng, H. D., & Suen, C. Y."Transformation-ring projection (TPR) algorithm and its VLSI implementation," International Journal of Pattern Recognition Artificial Intelligence, Vol. 5(2), pp.25–56, 1991.
37. Tang, Y. Y., Li, B. F., Ma, H., & Liu, J."Ring-projection-wavelet fractal signatures: a novel approach to feature extraction," IEEE Transaction on Circuits System: Analog and Digital Signal Processing, Vol.45 (8), pp.1130-1134, 1998.
38. Perfilieva, I. "Fuzzy transforms." Transactions on Rough Sets II, Springer Berlin, Heidelberg, Vol.3135, pp.63-81, 2004.

39. Perfilieva, I. ”Fuzzy Transforms: theory and applications”, Fuzzy Sets and Systems, Vol.157(8), pp.993–1023. 2006.
40. Di Martino, F., Loia, V., Perfilieva, I., & Sessa, S.”An image coding/decoding method based on direct and inverse fuzzy transforms.” International Journal of Approximate Reasoning, Vol.48 (1), pp.110-131, 2008.
41. Novák, V., Perfilieva, I., & Mockor, J. “Mathematical principles of fuzzy logic” Springer Science & Business Media, Vol. 517, 2012.
42. Pal, N. R. & Pal, S. K. “Object-background segmentation using new definitions of entropy”, IEE Proceeding E (Computers and Digital Technique), Vol.136 (4), pp.284-295, 1989.
43. Wang, X., Zhang, X., Li, Z., & Wang, S. “A DWT-DCT based passive forensics method for copy-move attacks”, 3rd IEEE International Conference on Multimedia Information Networking and Security, pp. 304-308, 2011.
44. http://www.micc.unii.it/ballan/research/image-forensics/.
45. Hashmi, M. F., & Keskar, A. G. “Block and Fuzzy Techniques Based Forensic Tool for Detection and Classification of Image Forgery”, Journal of Electrical Engineering and Technology, Vol.10 (4), pp.1886-1898 , 2015.
46. Pan, X., Lyu, S. “Region duplication detection using image feature matching” IEEE Transaction on Information Forensics and Security, Vol.5 (4), pp.857-867, 2010.
47. Heikkila, M., & Pietikainen, M. “A texture-based method for modeling the background and detecting moving objects”, IEEE transactions on pattern analysis and machine intelligence, Vol.28(4), pp. 657–662, 2006
48. Sertel, O., Kong, J., Shimada, H., Catalyurek, U. V., Saltz, J. H., & Gurcan, M. N. “Computer-aided prognosis of neuroblastoma on whole-slide images: Classification of stromal development”, Pattern recognition, Vol. 42(6), pp.1093–1103, 2009.